REMARKS

Claims 1-40 are pending in the present application. Claims 7, 13, 18, 19, 23, 30, 32, 37 and 38 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness

A. The Examiner rejected Claims 1-3, 5-8, 10-14, 17-26, 28-33 and 36-40 under 35 U.S.C. § 103 as being unpatentable over Muftic (US 5,850,442) in view of Applicant's own admissions, and further in view of Rankl (Smart Card Handbook © 1997). This rejection is respectfully traversed.

With respect to Claim 1, Applicants will first show that the Examiner's reasoning in combining the references and applying the teachings of such combination is logically inconsistent and therefore in error. Applicants will then show that even with such inconsistent reasoning, there are still missing claimed elements not taught or suggested by the cited references and thus the Examiner has failed to establish a prima facie showing of obviousness. If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

(i) Inconsistent Application of the Teachings of the Cited Muftic Reference re: Claim 1

In rejecting Claim 1, the Examiner makes the following statements regarding the teachings of Muftic:

(a) Muftic discloses "receiving, prior to the transaction, a secret *master key* from a third party... (see at least Abstract, Summary of the Invention, Fig 16: "smart token/certificate", associated text" (emphasis added by Applicants)

(b) Muftic discloses "retrieving the *master key* (retrieving unique client information)" (emphasis added by Applicants)

(c) "Although Muftic does disclose hashing a message digest, Muftic does not specifically disclose a *master key*" (emphasis added by Applicants)

Applicants show error in this analysis. First, Muftic's smart token/certificate is alleged to be the master key. Then, Muftic's unique client information is alleged to be the master key. Then, the Examiner acknowledges that Muftic does *not* disclose a master key. Applicants urge the last position (c) to in fact be the correct one – that Muftic does *not* disclose a master key.

This conclusion is evidenced by the fact that statement (a) cannot be true since the Muftic smart token/certificate is stated to be the smart card itself (Muftic column 1, line 20; column 10, lines 26-30), and there is no third party that stores a copy of the smart card. Claim 1 expressly requires that a copy of the master key (alleged by the Examiner to be the smart token, which per the teachings of Muftic is a smart card) is stored by a third party. Nor is statement (b), which equates "retrieving unique client information" to be the same as "retrieving the master key", correct. Muftic's unique client information is stated by the Examiner to be taught by Muftic's Figure 10 with respect to steps 1040 and 1060. Applicants urge that this Figure 10 and accompanying text describes a process for placing a customer order (column 13, lines 28-39). This unique client information is not received, prior to the transaction, from a third party as expressly recited in Claim 1 with respect to the claimed master key. Therefore, it is shown that an allegation that Muftic's unique client information reads on the claimed master key is incorrect. Thus, as allegations (a) and (b) are both erroneous, it logically follows – and as acknowledged by the Examiner – that Muftic 'does not specifically disclose a master key' (first full paragraph on page 4 of the present Office Action dated 9/22/2004).

Another inconsistency regarding the rejection of Claim 1 will now be shown. The Examiner states that Muftic teaches "creating the digest by hashing the unique client information and the master key (see at least C2, L38-41)". The Examiner then states in the next full paragraph "Muftic does not specifically disclose a master key, hashing a master key with customer information". These two statements are shown to be logically inconsistent, in that in the first instance it is alleged that the cited Muftic reference teaches *hashing unique client information and the master key*, and then in the second instance it is acknowledged that the cited Muftic reference does not disclose *hashing a master key with customer information*. In any event, Applicants urge that the passage

cited by the Examiner as teaching hashing unique client information and a master key instead states the following (Muftic column 2, lines 38-41):

> "In modern implementations, a message digest is created using a cryptographically strong one way hash function based on the message text and the message digest operates like a CRC check sum."

Applicants urge that while this passage may make mention of creating a message digest using a one-way hash function that is based on a message text, such one-way hash function does not teach or otherwise suggest *hashing two items in the creation of a digest*, and in particular does not teach or suggest "creating the digest by hashing the unique client information and the master key" (emphasis added by Applicants).

(ii) Claim 1 Missing Features

Specifically with respect to Claim 1, Applicants will now show that there are numerous claimed features not taught or suggested by any of the cited references. To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974) (emphasis added by Applicants).

(a) There is no teaching or suggestion of the claimed master key (the master key being defined to be a key that remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key). As established above in the Inconsistent Application of the Cited Mustic Reference, Mustic does not teach or suggest the claimed master key. The cited Rankl reference also does not disclose any such master key. The Examiner alleges that Rankl clearly discloses hashing consumer data with the smart card unique key at Section 4.3 and Figure 4.23. Applicants urge that while the teaching in Section 4.3 is with respect to hashing, it describes a one-way hash function which derives a fixed-length value from a variable-length document (page 83, second paragraph in Section 4.3). There is no teaching or suggestion of any type of master key, either as a part of the hash function or otherwise. The cited figure at Figure 4.23 is with respect to generation of a random number. While this random number generation technique does appear to use a card specific key, there is no teaching,

suggestion or other indication that this card specific key remains unchanged and is kept secret, is not altered after the transaction, with a third party storing a copy of this key, as expressly required by Claim 1. Thus, it is shown that the cited Rankl reference similarly does not teach or suggest the claimed master key as it is defined in Claim 1, or the use a master key as a part of a hash function, as expressly required by Claim 1.

(b) None of the cited references teach or suggest the claimed step of creating a digest by hashing unique client information and the master key. Initially, since there is no teaching or suggestion of the claimed master key, it necessarily follows that there is no teaching or suggestion of performing an operation such as creating a digest by hashing unique client information and the (missing) master key. Secondly, Applicants have shown above in the Inconsistence Application of the Mustic cited reference that Mustic does not teach or suggest this claimed step. The cited Rankl similarly does not teach hashing two items – customer information and a master key – to create a digest. Rather, it teaches (i) deriving a fixed length value from a variable length document (page 83, second paragraph in Section 4.3), and the use of a key to generate a random number (Figure 4.23). Thus, it has been shown that none of the cited references teach or suggest the claimed step of "creating the digest by hashing the unique client information and the master key".

(c) None of the cited references teach or suggest the claimed step of returning the digest (created by hashing unique client information and a master key) and the unique client information (used by the hashing process to create the digest that is returned) to the requestor. The Examiner alleges that this step is taught by Muftic's Figure 10 and element 1060. Applicants urge that this cited passage merely teaches that a user digitally signs an order form and sends it to a server (column 13, lines 36-39). There is no teaching or suggestion that this step includes returning a digest that was created by hashing unique client information and a master key, as expressly recited in Claim 1.

In conclusion regarding Claim 1, Applicants have shown numerous inconsistent interpretations per the teachings of the cited references. Applicants have further shown

numerous claimed steps/features not taught or suggested by the cited references. As all of the claim limitations must be taught or suggested by the prior art in order to establish a prima facie showing of obviousness (MPEP 2143.03), it is shown that a prima facie case of obviousness has not been established with respect to Claim 1.

Applicants initially traverse the rejection of Claims 2-3 and 5-7 for reasons given above regarding Claim 1, of which these Claims 2-3 and 5-7 depend upon.

Further with respect to Claim 2, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information". In rejecting Claim 2, the Examiner states that this is taught by Muflic's seller's ID shown in Figure 16. Applicants urge that this seller's ID (shown in Muflic's Figure 16, box 1620) is described to be an electronic ID that a user fills in to electronic charge slip when making a purchase (Muflic column 14, lines 40-42). In contrast, the claimed unique requestor information as recited in Claim 2 is *a part of a request for a digest from a requestor*. In addition, Claim 2 goes on to state that as a part of creating this requested digest, *the unique requestor information is hashed*. The teachings of Muflic are thus shown to be different for at least two reasons. First, the seller's ID is not part of a request for a digest from a requester, but is rather a manual user input value. Second, this seller's ID is not hashed when creating a digest. Thus, Claim 2 is further shown to not be obvious in view of the cited references as there are additional claimed features not taught or suggested by the cited references.

Further with respect to Claim 3, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the request includes unique merchant information which is used to access the master key". The Examiner acknowledges that the teachings of the cited Muflic reference are lacking in this regard, but states "it would have been obvious to one of ordinary skilled in the art at the time the invention was made to ensure that a request for billing digest would include unique merchant information that would dictate which master key the client system will fetch (i.e. Visa, MasterCard, AMEX, etc.). This would be inherent in the system, in order to allow it to properly match account holders and financial institutions". Applicants show twofold error in such assertion. First, inherency is not a proper basis for rejecting claims under 35 USC 103.

Rather, inherency is a concept to be used in 35 USC 102 rejections[1]. Second, Claim 3 expressly states that the unique merchant information (included as a part of the digest request) is used to access the master key. None of the cited references teach or suggest such use of unique merchant information, nor has the Examiner alleged any such teaching or suggestion of such use of unique merchant information. Thus, Claim 3 is further shown to have been erroneously rejected as a prima facie showing of obviousness has not been established.

Further with respect to Claim 5, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein creating the digest by hashing is performed by a smart card", where the creation of the digest is defined to be "creating the digest by hashing the unique client information and the master key". In rejecting Claim 5, the Examiner states that this claimed feature is taught by Muflic at column 4, lines 33-43; and Muflic Figure 3 with associated text. Applicants show error in such assertion as follows. Muflic states at column 4, lines 33-43:

> "As advances in technology permit continued increases in the degree of miniaturization of electronic components, smart cards have been developed which include a processor and/or memory built into a transport medium the size of a typical credit card. The processors in these cards can be programmed like any other computer to perform desired functions. Smart card readers are known which permit one to both read the contents of a smart card, but also to interact with the smart card to change its contents and to accomplish cooperative functions which can range from the simple to the sophisticated."

Applicants urge that this generalized statement regarding advances in smart card technology does not teach or otherwise suggest the specific features of Claim 5, such as creating a digest by a smart card, or hashing the unique client information and the master key by a smart card. As to Muflic's Figure 3 and associated text, Applicants urge that Muflic's Figure 3 does not even show a smart card or any associated operations that a smart card can perform. At best, it shows the existence of a smart card reader attached to

[1] Under section 102(b), anticipation requires that the prior art reference disclose, either expressly or under the principles of inherency, every limitation of the claim. In re King, 801 F.2d at 1326, 231 USPQ at 138; RCA Corp. v. Applied Digital Data Sys., Inc., 730 F.2d 1440, 1444, 221 USPQ 385, 388 (Fed. Cir.), cert. dismissed, 468 U.S. 1228 (1984).

a computer system. As to the text associated with Figure 3, such text states at column 10, lines 23-55:

> "FIG. 3 is an illustration of a computer incorporating smart token hardware which can be used for running either client or server software. In this exemplary illustration, the computer is equipped with the usual display 300, keyboard 330, mouse 340 and drives 320. *In addition, the computer is equipped with card reader 350 which will both read and write smart tokens such as smart cards or PCMCIA cards. Preferably, the cards are smart cards and card readers both read/write smart cards.* Although the term "reader" is used, it is to be understood that the term, as used herein, is intended to cover the writing of smart tokens as a necessary and inherent part of a "reader". Card reader 350 is illustrated as connected to the computer over cable 360 which connects to a port on the computer, such as an RS 232 port or via any other port or by a wireless connection. Card readers may be external devices connected to computers, as illustrated in FIG. 1, or they may be built in to other devices such as CPU 310, telephones, vending machines, or almost any computer equipped device.
> Although card reader 350 is equipped with a slot 370 for insertion of a smart card, smart card readers are also available which remotely sense the presence of a smart card in the vicinity of the reader and communicate with the smart card utilizing wireless technologies. In some such remote sensing card readers, the card readers broadcast an RF energy signal which is detected by the smart card and a response is sent from the smart card back to the remote sensing card reader. An interchange of data may then occur in both directions over the wireless link between the smart card and the reader. Some card readers are equipped with a keypad and display."

As can be seen, this passage merely describes an ability to read and write to a smart card, either by a reader or using RF wireless technology. There is no discussion of particular functionality that such a smart card performs, and in particular there is no teaching or suggestion of the specific features of Claim 5, such as creating a digest by a smart card, or hashing the unique client information and the master key by a smart card. Thus, Claim 5 is further shown to have been erroneously rejected as there are further missing claimed features not taught or suggested by the cited references.

With respect to Claim 6, Applicants urge that none of the cited references teach or suggest the claimed step of "encrypting the unique client information prior to retrieving

the unique client information". The Examiner admits that this step is not taught by any of the cited references, but states that it would just be common sense to encrypt client information to prevent unauthorized access or capture. Applicants urge that such common sense basis for rejection under 35 USC 103 is contrary to judicial requirements in establishing obviousness. Although a device may be capable of being modified to run the way [the patent applicant's] apparatus is claimed, there must be a suggestion or motivation *in the reference* to do so. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990) (emphasis added by Applicants). Applicants urge that there is no such suggestion for encrypting the client information *prior to its retrieval*. The only suggestion for such encryption prior to retrieval comes from Applicants' own disclosure and claims, which is improper hindsight analysis. This can further be seen by Muflic's teaching of a user inputting information in an order form (Muflic Figure 10, box 1040), which is alleged by the Examiner to be equivalent to the claimed unique client information. It is not seen how user information that is manually entered in an electronic order form can be encrypted *prior to retrieving such user information*, as expressly recited in Claim 6. Is the user alleged to be encrypting the data prior to entry into the terminal? Thus, Claim 6 is further shown to have been erroneously rejected as there is at least one additional missing claimed step not taught or suggested by the cited references.

Further with respect to Claim 7, such claim recites further details of the unique requestor information recited in Claim 2, and Claim 7 has been amended accordingly to depend upon Claim 2. In rejecting Claim 7, the Examiner points to the teachings of Muftic at Figure 13 and the associated text. Applicants urge that the amendment to Claim 7 further distinguishes the invention recited therein from the teachings of the cited Muftic reference, in that Claim 7 recites that the details of the unique requestor information *are a part of the unique requestor information that is hashed* (per Claim 2) when creating the digest. The teachings associated with Muftic Figure 13 merely states that the seller exchanges the credit card slip for the face amount less a service fee. Thus, the seller gets immediate cash (column 14, lines15-17). The teachings of Muftic do not teach or otherwise suggest the details of the unique requestor information recited in Claim 7, or the hashing of this information as a part of creating the digest. Thus, it is

shown that Claim 7 is not obvious in view of the cited references as there are numerous claimed features not taught or suggested by such references.

With respect to independent Claim 8, Applicants urge that none of the cited references teach or suggest (1) receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, (2) creating a billing digest by hashing (i) unique client information, (ii) a master key and (iii) the unique merchant information onboard the smart card; or (3) passing (i) the billing digest, (ii) the unique merchant information and (iii) the unique client information to the requestor. In rejecting Claim 8, the Examiner relies upon the same reasoning given regarding Claim 1 in rejecting Claim 8. Applicants show that the Examiner has thus failed to establish a prima facie case of obviousness, as *Claim 8 recites additional features not recited in Claim 1*. Specifically, Claim 8 recites that a data transmission including *unique merchant information is received into a smart card*. Claim 1 is silent as to any type of merchant information, such as receiving such merchant information into a smart card. Claim 8 also recites that the billing digest is created by hashing unique merchant information onboard the smart card. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as hashing unique merchant information onboard the smart card. Claim 8 also recites that the unique merchant information is passed to the requestor. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as passing the unique merchant information to the requestor. Thus, it is shown that Claim 8 is of different scope than Claim 1, and therefore the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 8 by merely relying on the reasoning given in rejecting Claim 1. Accordingly, as a prima facie case of obviousness has not been established by the Examiner, the burden has not shifted to Applicants to rebut an obviousness assertion[2].

Applicants traverse the rejection of dependent Claim10 for reasons given above with respect to Claim 8 (of which Claim 10 depends upon).

[2] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id.

With respect to independent Claim 11, Applicants urge that none of the cited references teach or suggest the claimed steps of (1) sending a data transmission to a smart card, wherein the data transmission includes unique merchant information, (2) receiving unique merchant information from the smart card; or (3) transmitting the unique merchant information from the smart card to a credit card issuer. In rejecting Claim 11, the Examiner relies upon the same reasoning given regarding Claim 1 in rejecting Claim 11. Applicants show that the Examiner has thus failed to establish a prima facie case of obviousness, as *Claim 11 recites additional features not recited in Claim 1*. Specifically, Claim 11 recites that a data transmission that includes *unique merchant information is sent to a smart card*. Claim 1 is silent as to any type of merchant information, such as sending such merchant information to a smart card. Claim 11 also recites that unique merchant information is received from the smart card. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as receiving unique merchant information from the smart card. Claim 11 also recites that the unique merchant information is transmitted from the smart card to a credit card issuer. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as transmitting the unique merchant information from the smart card to a credit card issuer. Thus, it is shown that Claim 11 is of different scope than Claim 1, and therefore the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 11 by merely relying on the reasoning given in rejecting Claim 1. Accordingly, as a prima facie case of obviousness has not been established by the Examiner, the burden has not shifted to Applicants to rebut an obviousness assertion.

Applicants traverse the rejection of dependent Claim 12 for reasons given above with respect to Claim 11 (of which Claim 12 depends upon).

With respect to independent Claim 13, Applicants urge that none of the cited references teach or suggest the claimed steps of (1) accessing the copy of the master key based on the unique client information, (2) creating an authorization digest by hashing the unique client information and the copy of the master key, or (3) comparing, by the third party, the authorization digest with the digest from the requestor. The cited Muftic reference merely teaches that authenticating an electronic message as to origin may involve validating a public key of a public key encryption pair of a user originating a

message by using digital signatures of one or more certification authorities (column 7, lines 32-40). As this authentication technique is different from the transaction processing described in Claim 13, it similarly follows that the steps recited in Claim 13 are not inherent in the teachings of the cited Muftic reference[3]. Thus, Claim 13 is shown to not be obvious in view of the cited references as there are numerous claimed features not taught or suggested by such references.

Applicants initially traverse the rejection of Claims 14 and 17-19 for similar reasons to those given above with respect to Claim 13 (of which Claims 14 and 17-19 depend upon).

Further with respect to Claim 14, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 2.

Further with respect to Claim 17, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 5.

Further with respect to Claim 19, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 7.

With respect to independent Claim 20, Applicants urge that none of the cited references teach or suggest the claimed step of "generating a billing digest in a customer's smart card, the billing digest being hashed from merchant information, customer information and a secret master key". As can be seen, this claimed step is directed to the generation of a billing digest, and such billing digest generation is done in a customer's smart card. In addition, this billing digest is hashed from (i) merchant information, (ii) customer information and (iii) a secret master key. None of the cited references teach generation of a billing digest in a smart card, or that the billing digest is hashed from the three explicitly listed items of merchant information, customer information and a secret master key. Thus, it is shown that Claim 20 has been erroneously rejected as there are several missing claimed features not taught or suggested by the cited references.

---

[3] "To establish inherency," the Federal Circuit recently stated, "the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *In re Robertson*, 169 F.3d 743, 745 [49 USPQ2d 1949] (Fed. Cir. 1999); see also *Continental Can Co. U.S.A., Inc. v. Monsanto Co.*, 948 F.2d 1264, 1268 [20 USPQ2d 1746] (Fed. Cir. 1991). Such inherency may not be established by "'probabilities or possibilities.'" *Continental Can*, 948 F.2d at 1269 (quoting In re Oelrich, 666 F.2d 578, 581 [212 USPQ 323] (C.C.P.A. 1981)).

With respect to independent Claim 21, Applicants urge that none of the cited references teach or suggest the claimed steps of (1) *indexing a secret master key to an account identifier for an account*, wherein the account is between a customer and a financial institution, or (2) passing transaction data through a third party, wherein the transaction data includes at least the customer account identifier, third party information and *a billing digest which is created from the customer account identifier, the third party information and the master key*. Nor has the Examiner alleged any such teaching or suggestion. Thus, a prima facie case of obviousness has not been established with respect to Claim 21 and the burden has not shifted to Applicants to rebut an obviousness assertion.

With respect to independent Claim 22, such claim recites details of the smart card used for conducting secure transactions. None of the cited references teach or suggest a smart card that comprises (1) a functional hashing algorithm, and (2) an executable application for invoking the functional hashing algorithm, where the functional hashing algorithm creates a digest from (i) the financial account information and (ii) the master key. In addition, none of the cited references teach or suggest a smart card that transmits (i) this created digest and (ii) the financial account information to a requestor. Nor has the Examiner alleged any such teaching or suggestion. Thus, a prima facie case of obviousness has not been established with respect to Claim 22 and the burden has not shifted to Applicants to rebut an obviousness assertion.

With respect to independent Claim 23, none of the cited references teach or suggest the claimed features of (1) a client smart card for creating a billing digest from (i) a resident client information, (ii) a resident secret master key and (iii) imported merchant information; or (2) creating an authorization digest from (i) the master key stored in the financial institution, (ii) the client information and (iii) the merchant information. As to missing claimed feature (1), none of the cited references teach or suggest creating a billing digest by a smart card, the billing digest being created from, among other things, *imported merchant information*. As to missing claimed feature (2), none of the cited references teach or suggest using the three items expressly identified therein – a master key, client information, and merchant information – in creating an authorization digest that is used to compare against a billing digest. Therefore, it is shown that Claim 23 is

not obvious in view of the cited references as there are numerous claimed features not taught or suggested by the cited references.

With respect to independent Claim 24 (and dependent Claims 25-26 and 28-31), Applicants initially traverse for similar reasons to those given above with respect to Claim 1.

Further with respect to Claim 25, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 2.

Further with respect to Claim 26, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 3.

Further with respect to Claim 28, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 5.

Further with respect to Claim 29, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 6.

Further with respect to Claim 30, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 7.

With respect to independent Claim 32 (and dependent Claims 33 and 36-38), Applicants initially traverse for similar reasons to those given above with respect to Claim 13.

Further with respect to Claim 33, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 2.

Further with respect to Claim 36, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 5.

Further with respect to Claim 38, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 7.

With respect to independent Claim 39, Applicants traverse for similar reasons to those given above with respect to Claim 1.

With respect to independent Claim 40, Applicants traverse for similar reasons to those given above with respect to Claim 8.

In summary, there are numerous claimed features recited as a part of the method, system and program product of the present invention related to secure transaction processing that are not taught or suggested by the cited reference, and thus as all of the

claim limitations are not taught or suggested by the cited references, a prima facie case of obviousness has not been established as required by MPEP 2143.03. In addition, as a prima facie case of obviousness has not been established, the burden has not shifted to Applicants to rebut an obviousness assertion.

B. The Examiner rejected Claims 4, 9, 15-16, 27 and 34-35 under 35 U.S.C. § 103 as being unpatentable over Muftic (US 5,850,442) in view of Applicant's own admissions, in view of Rankl (Smart Card Handbook © 1997), and further in view of Nguyen et al., (US Patent 5,931,917). This rejection is respectfully traversed.

Applicants traverse the rejection of Claims 4 and 27 for similar reasons to those given above with respect to Claim 1, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 1.

Applicants traverse the rejection of Claim 9 for similar reasons to those given above with respect to Claim 8, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 8.

Applicants traverse the rejection of Claims 15-16 and 34-35 for similar reasons to those given above with respect to Claim 13, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 13.

Further with respect to Claims 16 and 35, Applicants urge that none of the cited references teach or suggest the claimed features of "accessing all previously used reference numbers associated with the unique client information; comparing the previously used reference numbers with the reference number contained in the unique client information; and returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information". Nor has the Examiner alleged any such teaching or suggestion. Thus, a prima facie case of obviousness has not been established with respect to Claims 16 and 35 and the burden has not shifted to Applicants to rebut an obviousness assertion.

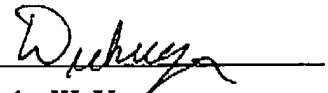
Therefore, the rejection of Claims 1-40 under 35 U.S.C. § 103 has been overcome.

II. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 1/21/05

Respectfully submitted,



Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants